Security Update: CISCO released 2 Critical and 9 High security advisories to address vulnerabilities in multiple products

CISCO released 2 Critical and 9 High security advisories to address vulnerabilities in multiple products

**Status Type**

Security Update

**Private**

Public

**Date and Time**

Monday, April 23, 2018 - 09:31

**Reason**

Security update

**Impact**

Cisco users

**WHAT HAPPENED**

CISCO released 2 Critical and 9 High security advisories to address vulnerabilities in multiple products.

**Advanced Users:** For a complete description of the vulnerabilities visit:

- Cisco UCS Director Virtual Machine Information Disclosure Vulnerability for End User Portal
Cisco StarOS Interface Forwarding Denial of Service Vulnerability:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180418-staros  

Cisco IOS XR Software UDP Broadcast Forwarding Denial of Service Vulnerability:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180418-iosxr  

Cisco Firepower Detection Engine Secure Sockets Layer Denial of Service Vulnerability:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180418-fpsnort  

Cisco Firepower 2100 Series Security Appliances IP Fragmentation Denial of Service Vulnerability:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180418-fp2100  

Cisco ASA Software, FTD Software, and AnyConnect Secure Mobility Client SAML Authentication Session Fixation Vulnerability:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180418-asaanyconnect  

Cisco Adaptive Security Appliance Application Layer Protocol Inspection Denial of Service Vulnerabilities:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180418-asa_inspect  

Cisco Adaptive Security Appliance TLS Denial of Service Vulnerability:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180418-asa3  

Cisco Adaptive Security Appliance Flow Creation Denial of Service Vulnerability:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180418-asa2  

Cisco Adaptive Security Appliance Virtual Private Network SSL Client Certificate Bypass Vulnerability:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180418-asa1

Affected Systems:

- Cisco WebEx Business Suite (WBS31) client builds prior to T31.23.2
- Cisco WebEx Business Suite (WBS32) client builds prior to T32.10
- Cisco WebEx Meetings with client builds prior to T32.10
- Cisco WebEx Meetings Server builds prior to 2.8 MR2
• Cisco Unified Computing System (UCS) Director releases 6.0 and 6.5

• Aggregation Services Router (ASR) 5700 Series

• Virtualized Packet Core?Distributed Instance (VPC?DI) System Software

• Virtualized Packet Core?Single Instance (VPC?SI) System Software

• Cisco IOS XR platforms running 6.3.1, 6.2.3, or earlier releases of Cisco IOS XR Software

• Adaptive Security Appliance (ASA) 5500-X Series Firewalls with FirePOWER Services

• Adaptive Security Appliance (ASA) 5500-X Series Next-Generation Firewalls

• Advanced Malware Protection (AMP) for Networks, 7000 Series Appliances

• Advanced Malware Protection (AMP) for Networks, 8000 Series Appliances

• Firepower 4100 Series Appliances

• FirePOWER 7000 Series Appliances

• FirePOWER 8000 Series Appliances

• Firepower 9300 Series Security Appliances

• Firepower Threat Defense for Integrated Services Routers (ISRs)
- Firepower Threat Defense Virtual for VMware

- Industrial Security Appliance 3000

- Sourcefire 3D System Appliances

- Cisco Firepower Threat Defense (FTD) Software Releases 6.2.1 and 6.2.2,

- 3000 Series Industrial Security Appliances (ISA)

- ASA 5500 Series Adaptive Security Appliances

- ASA 5500-X Series Next-Generation Firewalls

- ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers

- Adaptive Security Virtual Appliance (ASAv)

- Firepower 2100 Series Security Appliance

- Firepower 9300 ASA Security Module

- FTD Virtual (FTDv)

**WHAT’S THE PROBLEM?**

A remote attacker could exploit some of these vulnerabilities to take control of an affected system.
WHAT DO I NEED TO DO?

Users and administrators are encouraged to review the above Cisco Security Advisory and apply the offered updates.

RELATED LINKS

- IT SECURITY at https://it.ucsf.edu/security [12]

GET IT HELP. Contact the Service Desk online, or phone 415.514.4100

Source URL: https://it.ucsf.edu/status/2018-04-23/cisco-released-2-critical-and-9-high-security-advisories-address-vulnerabilities

Links:
[12] https://it.ucsf.edu/security